(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 583 316 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
18.04.2007 Bulletin 2007/16

(51) Int Cl.:
H04L 29/06 (2006.01) *H04L 12/46* (2006.01)

(21) Application number: **05101072.6**

(22) Date of filing: **14.02.2005**

(54) Secure transparent virtual private networks

Sichere und transparente virtuelle Privatnetzwerke

Réseaux privés virtuels sûrs et transparents

(84) Designated Contracting States:
DE FR GB IE

(30) Priority: **31.03.2004 US 813990**

(43) Date of publication of application:
05.10.2005 Bulletin 2005/40

(73) Proprietor: **NOVELL, INC.**
Provo,
Utah 84606-6194 (US)

(72) Inventors:
- **Ackerman, Mark D.**
  Eagle Mountain, Utah 84043 (US)
- **Ebrahimi, Hashem Mohammad**
  Salt Lake City, Utah 84108 (US)
- **Amin, Baber**
  Provo, Utah 84601 (US)

(74) Representative: **Hanna, Peter William Derek**
Hanna, Moore & Curley
13 Lower Lad Lane
Dublin 2 (IE)

(56) References cited:
EP-A- 1 304 830 **WO-A-02/15514**

- **Retrieved from the Internet: URL:HTTP://MSDN.MICROSOFT.COM/WORKSHOP/SERVER/FEATURE/VPNOVW.ASP> [retrieved on 1999-06-21]**

EP 1 583 316 B1

Description

Field of the Invention

[0001] The invention relates generally to network security, and more specifically to techniques for managing Virtual Private Network (VPN) communications.

Background of the Invention

[0002] The need for creating secure logical networks over public and insecure communication lines, such as the Internet, continues to grow. Organizations desire and many times require secure communications with remote clients or services. As a practical matter, dedicated communication lines and equipment are not viable options, since these are unnecessarily expensive and require ongoing maintenance and support. Thus, organizations have opted for a less expensive option and an easier option to implement and deploy. This option is referred to as a Virtual Private Network (VPN).

[0003] A VPN uses an insecure network (e.g., Internet or public telecommunications infrastructure) for providing secure communications between remote clients or services. A VPN requires participants to have a common infrastructure to support common encryption, decryption, security, and certain protocols. Data is encrypted from one participant and tunnelled using a secure protocol to another participant, where that data is decrypted and consumed. In some cases, even the address of the participants in a VPN is encrypted.

[0004] With VPN techniques there are local computing environments associated with local clients or services and a remote computing environments associated with remote clients of services. Conventionally, each local client needs to support VPN communications and directly establish secure communications (e.g., Secure Sockets Layer (SSL) or Transport Layer Security (TLS)) with a VPN server. This means each local client needs client-side software and a custom configuration in order to participate in a desired VPN with a remote client or service.

[0005] As is readily apparent, implementation of conventional VPN techniques within local networking environments can be challenging and time consuming, since each client of the local environment needs to be configured, maintained, and supported. However, often there is little concern with the security of communications being compromised within a local and trusted networking environment.

[0006] That is, security concerns are mainly associated with specific communications exiting and coming into the local networking environment over the insecure network connection (e.g., Internet). Thus, managing VPN techniques at each individual local client or service within the local networking environment is excessive and not necessary in order to ensure proper security. In other words, a single local service could ensure that all local clients participating within a VPN distribute and receive secure communications over the insecure network with desired remote clients or services. In this manner, clients or services can participate in a VPN via the service without having any individual and specific configuration, support, or maintenance being required.

[0007] Another drawback to traditional VPN techniques is that caching of data communicated during a VPN session is not available. This means that clients, who manage their own VPN session experience slower communication rates with their desired remote clients or services. Thus, there is a need for accelerating data delivery via local caching to local clients during VPN sessions.

[0008] Thus, improved techniques for transparently administering VPNs are needed.

[0009] WO-02/15514-A (Cyber IQ Systems) describes a VPN device clustering system that connects two or more VPN devices on one side of a virtual private network to a similarly clustered system of two or more VPN devices on the other side of a virtual private network. The VPN device clustering system typically includes a plurality of clustering units for redundancy that avoids difficulties that arise with a single point of failure. For example two clustering units may be used in an active-passive high-availability configuration. Clients are pre-configured to participate in a VPN communication with one another. The specific destination address for the target VPN is actually unassigned by the client or is associated with a generic pool; a proper servicing VPN device is then dynamically assigned within the target client's environment. Thus, specific assignments of VPN devices are not known to clients, but the VPN communications are known and pre-configured in the clients.

[0010] EP-A-1,304,830 (Stonesoft Corp.) describes centralized VPN management of a plurality of VPN sites by means of a VPN Information Provider (VIP). Management of a VPN device is distributed so that at least part of the VPN configuration is centrally managed without giving away control of the firewall rulebase or other critical local configuration used in the VPN device.

Summary of the Invention

[0011] The present invention provides methods and systems for managing a Virtual Private Network (VPN) in accordance with claims which follow. In various embodiments of the invention, techniques are presented for transparently administering a VPN. A VPN of this invention includes local clients or services, a local transparent VPN service, a remote transparent VPN service, and remote clients or services.

[0012] The local transparent VPN service receives communications directed by local clients or services to pre- defined ports. These ports are reserved or associated with VPN communications. When a local client directs a communication to one of these ports, a switch or router relays the communication to the local transparent VPN service for processing. The local transparent VPN

service inspects the communication for purposes of determining if the communication can be satisfied from data residing in local cache, and if so such data is delivered immediately to the initial requesting local client from the local cache.

[0013] If the communication can not be satisfied from the local cache, the n the local transparent VPN service identifies the specific VPN and remote client or service for which the communication is directed, translates the communication and any addresses of the participants appropriately and forwards the encrypted communication via SSL or TLS to a remote transparent VPN service, which performs features similar to the local transparent VPN service for the remote client.

Brief Description of the Drawings

[0014]

FIG. 1 is a diagram representing an architectural layout for a Virtual Private Network (VPN) managing system;

FIG. 2 is a flowchart representing a method for managing VPN communications;

FIG. 3 is a flowchart representing another method for managing VPN communications; and

FIG. 4 is a diagram representing a VPN managing system.

Detailed Description of the Invention

[0015] As used herein and below a " client" is an electronic application, " service", proxy, a computing device, or system which may be automated or may be manually interacted with by an end-user.

[0016] The phrases " local networking environment" and " external (remote) networking environment are presented herein and below. Local networking environment refers to physical or logical network devices and services which are configured to be local to the clients and which interface with the local clients. This does not mean that any particular local networking environment of a particular local client physically resides in the same geographic location of the local client or proximately resides within the same geographic location of the local client, although in some embodiments this can be the case. Local networking environments can be dispersed geographically from the physical location of the local client and form a logical local networking environment of the local client. An external networking environment is a network which is not considered local to the local client. A remote service is associated with external or remote networking environments, these external or remote networking environments are considered external and remote vis-à-vis a local client's networking environment. Moreover, the terms local and remote or external are relative terms and depending upon who is performing any particular transaction. Thus, a remote client can have a local network environment with respect to the remote client.

[0017] Secure communications refer to communications that require specific secure protocols (e.g., SSL, TLS, etc.), which are communicated over predefined ports (e.g., 443, etc.) associated with communication devices. Secure communications may also refer to any form of encryption or custom encryption and agreed upon protocol that is used to mutually establish secure communications between two or more entities. Thus, in many cases data communication using secure communications requires encryption. In some instances this encryption uses Public and Private Key Infrastructure (PKI) techniques and which may also use digital certificates and digital signatures. Insecure communications refer to communications that use insecure protocols (e.g. HTTP, etc.) and which use different defined ports (e.g., 80, etc.) of communication devices from that which are used with secure communications. Generally, insecure communications will also not include encryption.

[0018] A VPN is a logical network where two or more clients or services interact over an insecure network (e.g., Internet) in a secure fashion. The secure fashion may entail using specific ports (e.g., 443, etc.), using mutually agreed upon protocols (e.g., SSL, TLS, custom protocols, etc.), and using mutually agreed upon encryption and decryption. Traditionally, a VPN requires each client to include configuration, secure protocols, keys, and the like which reside on each client participating within a VPN. This is not the case with the teachings presented herein. A local transparent VPN service acts on behalf of a plurality of clients within local networking environments in order to manage VPN traffic. Remote clients and services are interacted with via the VPN through a remote transparent VPN service.

[0019] Data acceleration refers to the ability to cache data in advance of a need or request for that data. Any conventional caching services and managers can be used in the caching techniques presented herein and below with embodiments of this invention. Thus, by way of example, a cache manager can determine when to flush certain data from a cache and determine when certain data residing within the cache is stale and needs refreshed or updated. Generally, data is accelerated with caching techniques because the cache resides closer to a client and houses needed data in memory which is more quickly referenced and accessed. Thus, if a request for particular data can be satisfied from a local cache, a requesting client experiences a faster response time for that data and it appears to the client as if the data has been accelerated to satisfy a data request.

[0020] Various embodiments of this invention can be implemented in existing network products and services. For example, in some embodiments, the techniques presented herein are implemented in whole or in part in the iChain ®, Border Manager ®, and Excelerator ® products distributed by Novell, Inc., of Provo, Utah.

[0021] Of course, the embodiments of the invention can be implemented in a variety of architectural plat-

forms, systems, or applications. For example, portions of this invention can be implemented in whole or in part in any distributed architecture platform, operating systems, proxy services, or browser/ client applications. Any particular architectural layout or imple mentation presented herein is provided for purposes of illustration and comprehension only and is not intended to limit the various aspects of the invention.

[0022] FIG. 1 is a diagram representing one example architectural layout 100 for a Virtual Private Network (VPN) managing system. The architecture 100 is implemented within a distributed client-server architecture. The purpose of the architecture 100 is to demonstrate how various entities can be configured and arranged for interacting and managing a VPN. In some cases, entities permit acceleration of data acquired via the VPN.

[0023] The architecture 100 includes one or more local clients 101A-101B, a local transparent VPN service 102, a remote transparent VPN service 103, and one or more remote clients/ services 104A-104B. It should me noted that the local clients 101A-101B may also be services. The local transparent VPN service 102 communicates directly with the remote transparent VPN service 103 over an insecure network (e.g., Internet) using secure communications, such as SSL, TLS, or any other mutually agreed upon protocol 110.

[0024] During operation of the entities within the architecture 100, the local clients 101A-101B are not pre-configured with VPN capabilities or specialized software for processing VPN communications. Instead, the local clients 101A-101B attempt to communicate with a specific remote client/ service 104A or 104B or a group of remote clients/ services 104A-104B. The local client 101A or 101B may or may not know that its communication with the desired remote client/ service 104A or 104B is being achieved securely via a VPN. For example, a forward or transparent proxy may detect local client 101A or 101B communications and direct those communications to the secure port (e.g., 443) associated with VPN traffic. The secure communication port is monitored by a router or switch (not shown in FIG. 1), which detects a destination address for a remote client/ service 104A or 104B communication that is associated with a VPN. This causes the router or switch to relay the communication to the local transparent VPN service 102.

[0025] The local transparent VPN service 102 inspects the intercepted communication and determines whether the information or data desired can be satisfied out of a local cache, and if so delivers that information or data to the local client 101 A or 101B from the local cache. In these situations, since the local transparent VPN service 102 acts as a transparent intermediary for the local clients 101A-101B, the local transparent VPN service 102 is capable of communicating with the remote transparent VPN service 103 in advance of any specific communication from one of the local clients 101A or 101 B, such that data can be pre-acquired and populated in the local cache, managed, and accessed by the local transparent VPN service 102.

[0026] Traditionally, VPN communications were not capable of being cached within local environments of clients, since the secure communications tunnels between clients prevented any other service acting on behalf of the client to cache desired data. However, with the teachings presented herein, clients 101A-101B and 104A-104B can experience accelerated data delivery during VPN communications.

[0027] If an intercepted VPN communication cannot be satisfied by a local cache, the local transparent VPN service 102 inspects the communication to determine the proper VPN being requested based on the addresses of the participants (e.g., local and remote clients or services 101A- 101B and 104A- 104B). This permits the local transparent VPN service 102 to identify a needed remote transparent VPN service 103 with which the local transparent VPN service 102 communicates.

[0028] Next, the local transparent VPN service 102 performs the needed encryption on the communication and optionally on the addresses of the participants. The encryption is based on the identified VPN associated with the participants and their addresses. The encrypted communication is then sent over the insecure network (e.g., Internet) using a secure communications protocol (e.g., SSL, TLS, any mutually agreed upon protocol, etc.).

[0029] The encrypted communication is detected on a secure port (e.g., 443) within the remote networking environment and, in manners similar to what was discussed above, is forwarded to the remote transparent VPN service 103. The remote transparent VPN service 103 decrypts the communication and addresses, if applicable, and forwards the communication to needed remote clients/ services 104A- 104B for processing.

[0030] The targeted remote client/ service 104A or 104B acts on the communication and generates a response which it directs to the local client 101 A or 101 B. This response is intercepted and directed to the remote secure communication port. There, the reply is intercepted again and relayed to the remote transparent VPN service 103, where it is encrypted and sent from the remote transparent VPN service 103 over the insecure network using a secure communications protocol (SSL or TLS 110) to the local transparent VPN service 102. The local transparent VPN service 102 can cache the response and its data within a local cache and delivers the response to the original requesting local client 101A or 101B.

[0031] The local transparent VPN service 102 and the remote transparent VPN service 103 communicate directly with one another over an insecure network using secure communications (e.g., protocols and/ or encryption and decryption). Each transparent VPN service 102 or 103 can service a plurality of clients or services 101A-101B and 104A- 104B which engage in VPN interactions. Thus, individual clients/ services 101A- 101B or 104A-104B need not be pre-configured, managed, and supported for VPN communications and still can benefit and

participate in VPNs with the teachings presented herein. Additionally, the clients/ services 101A-101B and 104A-104B can, with some embodiments, experience accelerated data deliver during a VPN session, since the transparent VPN services 102 or 103 can cache data in advance of a need to satisfy a received communication.

[0032] FIG. 2 is a flowchart of one method 200 for managing VPN communications. The method 200 is implemented in a computer readable medium and is accessible over a network. In one embodiment, the method 200 is implemented as a local transparent VPN service, which is designed to interact with one or more local clients or services and designed to securely interact with a remote transparent VPN over an insecure network. The remote transparent VPN service is another processing instance of the method 200, which resides and processes in an external or remote networking environment. The processing of the method 200 is referred to as a " local transparent VPN service" herein and below.

[0033] In one embodiment, the transparent VPN service is a service which the local clients or services are not aware of That is, local clients are not pre-configured to directly interact with the local transparent VPN service. In this situation a router, switch, or proxy can be used to forward communications from the local clients to the local transparent VPN service. In a different embodiment, the local clients are configured to directly send VPN communications to the local transparent VPN service.

[0034] A local client or service issues a communication request for a remote client of service. This communication is directed or redirected on behalf of the local client to a specific secure communications port (e.g., 443, etc.), where a router or switch relays or forwards the communication to the local transparent VPN service. Accordingly, at 210, the local transparent VPN service receives a communication from a local client, which is directed to a remote client or service. Further, at 211, this communication is detected, in some embodiments, based on the local client's attempt to access a defined port with the communication.

[0035] The communications can also be based on the type of communication taking place. For example, in some embodiments, maybe only File Transfer Protocol (FTP) or Transmission Control Protocol (TCP) communication types are inspected and processed by the local transparent VPN service. Accordingly, processing can be based on the use of a specific communication port, based on a specific type of communication (e.g., FTP, TCP, etc.), or based on a combination of a specific communication port and a specific type of communication.

[0036] At 220, the local transparent VPN service receives the communication and identifies the VPN associated with the communication. To do this, the local transparent VPN service inspects the address or identity of the local client and the address or identity of the remote client or service. This information is looked up in a table or other data structure to acquire the identity of the specific VPN used between the local client and the remote client or service.

[0037] Once the specific VPN is identified, the local transparent VPN service can acquire the encryption, key, and any certificate information necessary to interact with a remote transparent VPN service at 221. The remote transparent VPN service is a remote processing instance of the local transparent VPN service. That is, the remote transparent VPN service is a local transparent VPN service with respect to the remote client or service.

[0038] In some embodiments, at 222, the original received communication is inspected by the local transparent VPN service for purposes of determining whether it can be satisfied from a local cache. In this way, the local transparent VPN service and the remote transparent VPN service interact with one another in advance and at different times than what may be requested by a local client and a remote client or service.

[0039] During these interactions, the local transparent VPN service acquires data associated with the remote client or service from the remote transparent VPN service and houses that data in a local cache that resides within the local networking environment of the local client and the local transparent VPN service. Thus, when the local client issues a communication request, the local transparent VPN service can inspect the local cache to determine if that communication can be satisfied locally. By doing this, the local client experiences accelerated data delivery during a VPN managed transaction. Conventionally, this has not been achievable.

[0040] In a like manner the remote transparent VPN service can acquire data from the local client via the local transparent VPN service and cache that data in a remote cache (local cache vis- à- vis the remote client or service and remote transparent VPN service), where that data can be used to accelerate data delivery to the remote client or service which interacts via the VPN with the local client.

[0041] At 230, the local transparent VPN service translates the original received communication and, optionally, any addresses of the parties involved (e.g., local and remote clients or services) into encrypted formats required by the VPN. That encrypted information is then sent using secure communications (e.g., protocols and/or encryption and decryption) to the remote transparent VPN service. The remote transparent VPN service receives that encrypted communication, decrypts it, identifies the address of the desired remote client or service, and forwards the decrypted version locally to that remote client or service. The remote client or service responds via a defined secure communication port (either directly or indirectly) within the remote networking environment. That response is relayed to the remote transparent VPN service, where it is translated and sent with secure communications to the local transparent VPN service.

[0042] Interactions between the local and remote transparent VPN services occur as long as the local and remote clients or services are interacting via the identified VPN. The transparent VPN services acts as intermedi-

aries for the local and remote clients or services. A single transparent VPN service can service a plurality of clients or services which are within the local networking environment of that transparent VPN service.

[0043] Conventionally, a VPN transaction required each client or service to be specifically configured, maintained, and supported for purposes of participating in VPN communications. With the teachings of this invention, this is no longer required since all clients or services of one environment can participate in a variety of VPN-defined communications with all clients or services of a different environment and all that is needed is a single transparent VPN service, which has an operational instance processing in each environment. Thus, two services can achieve what has previously required modification to all clients and services participating in VPN- defined communications.

[0044] In fact, in some embodiments, the local and remote clients are not even aware of the secure communications and the VPN being used in between their communications with one another. Thus, as far as the clients are concerned they believe that they are communicating insecurely with one another, when in fact communication between them is occurring via a VPN over a public or otherwise insecure network via the transparent VPN services.

[0045] FIG. 3 is a flowchart of another method 300 for managing VPN communications. The method is implemented in a computer readable medium and is accessible over any network or combination of networks. Similar, to the method 200 of FIG. 2 above, the method 300 can be viewed as a local transparent VPN service that interacts with another processing instance of itself (defined as a remote transparent VPN service) over a network. The two processing instances of the transparent VPN services manage VPN communications for a plurality of clients and services.

[0046] At 310, the local transparent VPN service receives an intercepted local client communication (can also be a local service). The communication is intercepted by detecting it on a predefined port which is monitored or listened to by the local transparent VPN service or which is monitored by a router or switch that automatically forwards communications to the local transparent VPN service.

[0047] The local transparent VPN service can be used to manage additional communications associated with a plurality of different local clients, as depicted at 321. That is, the local transparent VPN service intercepts and manages VPN communications for local clients or services which are within the local networking environment of the local transparent VPN service.

[0048] At 320, the intercepted communication from the local client is relayed and received for processing by the local transparent VPN service. At 330, that communication is inspect to determine if it can be satisfied from local cache being managed and maintained by the local transparent VPN service.

[0049] The local transparent VPN service interacts with its counterpart, the remote transparent VPN service, using secure communications (e.g., protocols (SSL, TLS, etc.) and/ or encryption and decryption). Thus, the local transparent VPN service can pre- acquire data from one or more remote clients or services via the remote transparent VPN service. Similarly, the remote transparent VPN service can reacquire data from one of more local clients of services via the local remote transparent VPN service. The data is stored and managed in caches, one cache local to the local client and another cache local to the remote client or service.

[0050] If at 330, the received communication can be satisfied from the cache, then, at 331, the local client is serviced with data from the local cache. In this manner, the local client can, in some instances, experience accelerated data delivery associated with VPN interactions. This has not conventionally been achievable. However, if at 330, the received communication cannot be satisfied from the local cache then, at 340, the proper remote transparent VPN service is located. The local transparent VPN service can interact with a plurality of remote transparent VPN services, so, at 340, the identity of the needed remote transparent VPN service is acquired based on the remote client or service for which the original communication is being directed.

[0051] The local transparent VPN service and the remote transparent VPN service interact with one another via secure communications, such as SSL or TLS. In some instances for added security digital certificates can be exchanged and in some instances the communications or certificates can be mutually or unilaterally digitally signed, as depicted at 341.

[0052] Once the identity of the remote transparent VPN service is known, the communication is translated (e.g., encrypted) and sent via the proper VPN to the target remote transparent VPN service, at 342. The translated communication is sent via secure communications (e.g., SSL or TLS). Once the encrypted communication is received by the remote transparent VPN service, it is decrypted and sent to the proper remote client or service for processing.

[0053] Once processed, the remote transparent VPN service intercepts the remote client's or service's response, encrypts it and sends it securely via the VPN using secure communications to the local transparent VPN service. The local transparent VPN service, decrypts it, optionally caches the data associated with it in local cache, and delivers it to the originally requesting local client.

[0054] The transparent VPN services act as VPN intermediaries or managers for VPN communications. This permits data during VPN communications to be cached and accelerated for deliver to clients or service and permits a plurality of clients or services to actively and beneficially participate in VPN communications without requiring individual maintenance, support, and configuration to achieve the same.

[0055] FIG. 4 is a diagram depicting a VPN managing system 400. The VPN managing system 400 is implemented in a computer readable or accessible medium and is accessible over any network or combination of networks. In some embodiments, portions of the VPN managing system 400 can be implemented using the techniques presented above with respect to method 200 or method 300 of FIGS 2- 3.

[0056] The VPN managing system 400 includes a local transparent VPN service 401 and a remote transparent VPN service 402. In another embodiment, the VPN managing system 400 includes a local transparent VPN service 401 and a local communication port 401A.

[0057] The VPN managing system 400 is operational in a local client environment and a remote client or service environment. Each separate environment can include one or more identical entities. For example, the local client environment can include local communication ports 401A, local routers or switches 401 B, and local cache 401C. At the same time, the remote client or service environment can include remote ports 402A, remote routers or switches 402B, and remote cache 402. In some embodiments, one or more entities may be omitted. Additionally, the environments need not be identically replicated, as is depicted in FIG. 4 for purposes of illustration.

[0058] The local client environment includes a plurality of clients or services 410. Each of these clients or services 410 can participate in VPN communications over an insecure network 415 with a plurality of remote clients or services 420, which reside in the remote client or service environment. The local and remote clients or services 410 and 420 do not need to be specifically configured to participate in VPN communications; rather, the details of VPN communications are managed by the two transparent VPN services 401 and 402. Each of the transparent VPN services 401 and 402 are capable of multiplexing, encrypting, or decrypting communications occurring between them and sending communications securely via SSL or TLS for purposes of effectuating a desired VPN. In fact, in many instances, the clients may be entirely unaware that they are communicating securely with other remote clients or services 420.

[0059] A local client 410 issues a communication to a specific secure communications port 401A. This can be achieved directly (e.g., forward proxy not shown in FIG. 4) or indirectly (e.g., transparent proxy not shown in FIG. 4). The local transparent VPN service 401 listens on that port for VPN activity. Alternatively, a local router or switch 401 B detects the activity and based on its type (e.g., FTP, TCP, etc.) or based on where it is headed (e.g., target remote client or service 420) relays or forwards the activity to the local transparent VPN service 401.

[0060] Once the local transparent VPN service 401 receives a communication associated with a VPN from a local client or service 410 which is destined for a remote client of service 420 over the insecure network 415, the local transparent VPN service 401 determines the identity of the remote transparent VPN service 402 with which it needs to interact over the desired VPN. Once this is known, the encrypting, decryption, certificate, keys, or multiplexing requirements can be established and the communication can be translated and sent over the insecure network 415 using secure communications (e.g., protocols and/ or encryption and decryption).

[0061] In some embodiments, the communication can be inspected by the local transparent VPN service 401 for purposes of determining whether it can be satisfied from contents of existing local cache 401C, and if it can be so satisfied, the local client's 410 original communication is immediately responded to with data residing in the local cache 401C. Thus, in some embodiments, client or service 410 and 420 can experience accelerated response time and data delivery, because of the caching abilities of the transparent VPN services 401 and 402. The caching is not limited to the local client environment, since, in some embodiments, the remote transparent VPN service 402 can perform caching using its remote cache 402C on behalf of its remote clients of services 420.

[0062] If a communication cannot be satisfied from cache 401C or 402C, then the appropriate transparent VPN service 401 or 402 encrypts and securely transmits the encrypted communication over the insecure network to its counterpart transparent VPN service 401 or 402. Here, the encrypted communication is decrypted or multiplexed and forwarded to the appropriate client or service 410 or 420 for processing and reply. The reply is then processed in the same manner as the communication was processed.

[0063] In some embodiments, the transparent VPN services 401 and 402 can interact with digital certificates and/ or via digital signatures. In fact, the desired level of security can be configured based on the needs of an organization. The services 401 and 402 interact with one another for purposes of achieving VPN communications on behalf of clients or services 410 and 420 of their environments. Moreover, in some instances, data is cached and provided for accelerated delivery. These benefits have not been achievable with conventional VPN techniques.

[0064] Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art will appreciate that any arrangement calculated to achieve the same purpose can be substituted for the specific embodiments shown. This disclosure is intended to cover all adaptations or variations of various embodiments of the invention. It is to be understood that the above description has been made in an illustrative fashion only. Combinations of the above embodiments, and other embodiments not specifically described herein will be apparent to one of ordinary skill in the art upon reviewing the above description. The scope of various embodiments of the invention includes any other applications in which the above structures and methods are used.

Claims

1. A computer-implemented method for managing Virtual Private Network (VPN) communications, comprising:

   receiving (210), at a local transparent VPN service (401), a communication from a local client (410) which is directed to a remote client (420) over an insecure network (415);
   identifying (220) a VPN associated with the communication;
   translating (230) the communication into an encrypted format for delivery within the VPN;
   sending (231) the translated communication from the local transparent VPN service (401) via the VPN to a remote transparent VPN service (402), which manages VPN traffic for the remote client by decrypting and supplying the translated communication to the remote client;
   characterized in that neither the local client (410) nor the remote client (420) is preconfigured with VPN capabilities or specialized software for processing VPN communications, and **in that** said receiving (210) comprises the steps of;
   detecting, at a forward or transparent proxy, router or switch (401B) the communication from the local client whenever the local client attempts to send the communication insecurely over a network to the remote client via a specific predefined communications port (401A);
   intercepting the detected communication and directing (211) it from the proxy, router or switch to the local transparent VPN service.

2. The method of claim 1 further comprising, interacting (221) with the remote transparent VPN service (402) to manage additional communications between the local client and the remote client via the VPN.

3. The method of claim 2 further comprising, caching (222) data received from the remote transparent VPN service (402) in a local cache for accelerated delivery to the local client (410).

4. The method of claim 1 wherein receiving (210) the communication further includes receiving the communication in at least one of a File Transfer Protocol (FTP) format and a Transmission Control Protocol (TCP) format.

5. The method of claim 1 further comprising, communicating with the remote transparent VPN service (402) over the insecure network (415) via Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

6. The method of claim 1, further comprising:

   inspecting (330) the communication for determining whether the communication is a request for data that resides in a local cache (401C), and if so, delivering (331) the data to the local client (410), and if not, locating (340) a remote transparent VPN service (402) associated with the VPN, and wherein the communication is translated (342) into formats used by the VPN and sent securely over an insecure network to the remote transparent VPN service for delivery (343) to the remote client (420).

7. The method of claim 6 wherein inspecting (330) further includes establishing (341) secure communications with the remote transparent VPN service (402) using at least one of Sockets Layer (SSL) and Transport Layer Security (TLS).

8. The method of claim 6 wherein inspecting (330) further includes identifying the remote transparent VPN service (402) as a service which is managing VPN traffic for the remote client (420).

9. The method of claim 6 further comprising:

   receiving a response communication from the remote client (420) via the remote transparent VPN service (402), if the communication had been sent via the VPN because it could not be satisfied from the local cache (401 C);
   translating the response based on the formats of the VPN; and
   delivering the translated response to the local client.

10. The method of claim 6 further comprising, managing (321) additional communications associated with the VPN from one or more different local clients (410) which are directed between one or more different remote clients (420), wherein the remote transparent VPN service (402) manages the additional communications on behalf of the one or more different remote clients.

11. The method of claim 6 wherein receiving further includes intercepting (310) the communication after detecting that the local client is transmitting the communication with a non-Hypertext Transfer Protocol (HTTP).

12. The method of claim 6 further comprising, interacting (341) with the remote transparent VPN service with mutually signed certificates that are exchanged between the local and the remote transparent VPN services during the interactions.

13. A Virtual Private Network (VPN) managing system (400), wherein neither local client(s) (410) nor remote client(s) (420) is/are preconfigured with VPN capabilities or specialized software for processing VPN communications, comprising:

    a local transparent VPN service (401);
    a local forward or transparent proxy, router or switch (401 B), adapted for detecting a communication from a local client whenever the local client attempts to send the communication insecurely over a network to a remote client via a specific predefined local communications port (401 A), and adapted to intercept the detected communication and to direct (211) it from the local proxy, router or switch to the local transparent VPN service;
    a remote transparent VPN service (402);
    a remote forward or transparent proxy, router or switch (402B), adapted for detecting a communication from a remote client whenever the remote client attempts to send the communication insecurely over the network to a local client via a specific predefined remote communications port (402A), and adapted to intercept the detected communication and to direct (211) it from the remote proxy, router or switch to the remote transparent VPN service.

14. The VPN managing system of claim 13, further comprising

    a local cache (401C);

    wherein local transparent VPN service (401) intercepts and manages VPN traffic on behalf of one or more local clients (410) and services communications of those local clients with data in the local cache (401C), if available, and if the data is not available in the local cache, the local transparent VPN service transmits the communications securely to the remote transparent VPN service for delivery and servicing by one or more remote clients (420) which the remote transparent VPN service (402) manages.

15. The VPN managing system of claim 13 wherein the local transparent VPN service (401) and the remote transparent VPN service (402) interact via at least one of Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

16. The VPN managing system of claim 13 wherein the local transparent VPN service (102,401) intercepts local VPN traffic on behalf of the one or more local clients (101,410) by inspecting Transmission Control Protocol (TCP) or File Transfer Protocol (FTP) communications originating from the one or more local clients.

17. The VPN managing system of claim 13 wherein communications between the local (102,401) and remote (103,402) transparent VPN services occur with mutually exchanged certificates.

18. The VPN managing system of claim 13, wherein the system resides on a server and services a plurality of local clients (410) associated with the VPN communications.

19. The VPN managing system of claim 13 wherein the system resides on a single client.

20. A computer program which when executing on a computer or computer network performs the method as claimed in any one of claims 1 to 12.

21. The computer program of claim 20, when stored on a machine-accessible medium.

Patentansprüche

1. Computer-implementiertes Verfahren zum Organisieren von Kommunikationen eines virtuellen Privatnetzes (VPN), umfassend:

    Empfangen (210) einer Kommunikation von einem lokalen Client (410), die zu einem fernen Client (420) gerichtet ist, über ein unsicheres Netz (415) bei einem lokalen transparenten VPN-Dienst (401);
    Identifizieren (220) eines der Kommunikation zugeordneten VPN;
    Übersetzen (230) der Kommunikation in ein verschlüsseltes Format zur Lieferung innerhalb des VPN;
    Senden (231) der übersetzten Kommunikation von dem lokalen transparenten VPN-Dienst (401) über das VPN zu einem fernen transparenten VPN-Dienst (402), der den VPN-Verkehr für den fernen Client organisiert durch Entschlüsseln und Zuführen der übersetzten Kommunikation zu dem fernen Client;
    dadurch gekennzeichnet, dass weder der lokale Client (410) noch der ferne Client (420) mit VPN-Fähigkeiten oder spezialisierter Software zum Verarbeiten von VPN-Kommunikationen vorkonfiguriert ist, und dass das Empfangen (210) die Schritte umfasst;
    Erfassen der Kommunikation von dem lokalen Client bei einem Weiterleitungs- oder Transparent-Proxy, Router oder einer entsprechenden Vermittlung (401B) jedes Mal, wenn der lokale Client versucht, Kommunikation in unsicherer Weise über ein Netz zu dem fernen Client über einen spezifizierten vordefinierten Kommunikationsanschluss (401A) zu senden;

Abfangen der erfassten Kommunikation und Richten (211) von ihr von dem Proxy, Router oder der Vermittlung zu dem lokalen transparenten VPN-Dienst.

2. Verfahren nach Anspruch 1, ferner das Interagieren (221) mit dem fernen transparenten VPN-Dienst (402) umfassend zum Organisieren zusätzlicher Kommunikationen zwischen dem lokalen Client und dem fernen Client über das VPN.

3. Verfahren nach Anspruch 2, ferner das Zwischenspeichern (222) von von dem fernen transparenten VPN-Dienst (402) empfangenen Daten in einem lokalen Cash- bzw. Zwischenspeicher zum beschleunigten Liefern zu dem lokalen Client (410) umfassend.

4. Verfahren nach Anspruch 1, wobei das Empfangen (210) der Kommunikation ferner das Empfangen der Kommunikation in mindestens einem von einem Dateienübertragungsprotokoll- bzw. File-Transfer-Protocol-Format (FTP-Format) und einem Sendesteuerprotokoll- bzw. Transmission-Control-Protocol-Format bzw. (TCP-Format) einschließt.

5. Verfahren nach Anspruch 1, ferner das Kommunizieren mit dem fernen transparenten VPN-Dienst (402) über das unsichere Netz (415) über die SSL-Schicht bzw. Secure-Sockets-Layer oder TLS bzw. Transportschichtsicherheit (TLS) umfassend.

6. Verfahren nach Anspruch 1, ferner umfassend:

Inspizieren (330) der Kommunikation in Bezug auf das Bestimmen, ob die Kommunikation eine Abfrage für Daten ist, die sich in einem lokalen Cash-Speicher befinden (401C), und wenn das der Fall ist, Liefern (331) der Daten zu dem lokalen Client (410), und wenn es nicht der Fall ist, Lokalisieren (340) eines fernen transparenten VPN-Dienstes (402), der dem VPN zugeordnet ist, und

wobei die Kommunikation in Formate übersetzt wird (342), die durch das VPN verwendet werden, und sicher über ein unsicheres Netz zu dem fernen transparenten VPN-Dienst gesendet werden zur Lieferung (343) an den fernen Client (420).

7. Verfahren nach Anspruch 6, wobei das Inspizieren (330) ferner das Einrichten (341) sicherer Kommunikationen mit dem fernen transparenten VPN-Dienst (402) unter Verwendung von mindestens einem von SSL bzw. Secure-Sockets-Layer (SSL) und TLS bzw. Transport-Layer-Security (TLS) einschließt.

8. Verfahren nach Anspruch 6, wobei das Inspizieren (330) ferner das Identifizieren des fernen transparenten VPN-Dienstes (402) als einen Dienst einschließt, der VPN-Verkehr für den fernen Client (420) organisiert.

9. Verfahren nach Anspruch 6, ferner umfassend:

Empfangen einer Antwort-Kommunikation von dem fernen Client (420) über den fernen transparenten VPN-Dienst (402), wenn die Kommunikation über das VPN gesendet worden ist, weil es von dem lokalen Cash (401C) nicht zufriedengestellt werden könnte;
Übersetzen der Antwort basierend auf den Formaten des VPN; und
Liefern der übersetzten Antwort an den lokalen Client.

10. Verfahren nach Anspruch 6, ferner das Organisieren (321) zusätzlicher, zwischen einem oder mehreren unterschiedlichen fernen Clients (420) gerichteter Kommunikationen, die dem VPN zugeordnet sind, von einem oder mehreren unterschiedlichen lokalen Clients (410) umfassend, wobei der ferne transparente VPN-Dienst (402) die zusätzlichen Kommunikationen anstelle des einen oder der mehreren unterschiedlichen fernen Clients organisiert.

11. Verfahren nach Anspruch 6, wobei das Empfangen ferner das Abfangen (310) der Kommunikation einschließt nach dem Erfassen, dass der lokale Client die Kommunikation nicht mit einem Hypertext-Transfer-Protocol (HTTP) sendet.

12. Verfahren nach Anspruch 6, ferner das Interagieren (341) mit dem fernen transparenten VPN-Dienst mit gegenseitig signierten Zertifikaten umfassend, die zwischen den lokalen und den fernen transparenten VPN-Diensten während der Interaktionen ausgetauscht werden.

13. Organisationssystem (400) eines virtuellen Privatnetzes (VPN), wobei weder ein oder mehrere lokale Clients (410) noch ein oder mehrere ferne Clients (420) mit VPN-Fähigkeiten oder spezialisierter Software zum Verarbeiten von VPN-Kommunikationen vorkonfiguriert sind, umfassend:

einen lokalen transparenten VPN-Dienst (401);
einen lokalen Weiterleitungs- oder Transparent-Proxy, Router oder eine entsprechende Vermittlung (401B), angepasst zum Erfassen einer Kommunikation von einem lokalen Client jedes Mal wenn der lokale Client versucht, die Kommunikation unsicher über ein Netz zu einem fernen Client über einen spezifisch vordefinierten lokalen Kommunikationsanschluss (401A) zu

senden, und angepasst zum Abfangen der erfassten Kommunikation und zum Richten (211) von ihr von dem lokalen Proxy, Router oder der Vermittlung zu dem lokalen transparenten VPN-Dienst;
einen fernen transparenten VPN-Dienst (402);
einen fernen Weiterleitungs- oder Transparent-Proxy, Router oder eine entsprechende Vermittlung (402B), angepasst zum Erfassen einer Kommunikation von einem fernen Client jedes Mal, wenn der ferne Client versucht, die Kommunikation unsicher über das Netz zu einem lokalen Client über einen spezifischen vordefinierten fernen Kommunikationsanschluss (402A) zu senden, und angepasst zum Abfangen der erfassten Kommunikation und zum Richten (211) von ihr von dem fernen Proxy, Router oder der Vermittlung zu dem fernen transparenten VPN-Dienst.

14. VPN-Organisationssystem nach Anspruch 13, ferner einen lokalen Zwischenspeicher bzw. Cash (401C) umfassend;
wobei der lokale transparente VPN-Dienst (401) VPN-Verkehr für einen oder mehrere lokale Clients (410) und Dienstekommunikationen von jenen lokalen Clients mit Daten im lokalen Cash-Speicher (401C) wenn verfügbar abfängt und organisiert, und wenn die Daten nicht in dem lokalen Cash-Speicher verfügbar sind, der lokale transparente VPN-Dienst die Kommunikationen sicher zu dem fernen transparenten VPN-Dienst übermittelt zum Liefern und Bedienen durch einen oder mehrere ferne Clients (420), der bzw. die den fernen transparenten VPN-Dienst (402) organisiert bzw. organisieren.

15. VPN-Organisationssystem nach Anspruch 13, wobei der lokale transparente VPN-Dienst (401) und der ferne transparente VPN-Dienst (402) über mindestens eines von Secure-Sockets-Layer (SSL) und Transport-Layer-Security (TLS) interagieren.

16. VPN-Organisationssystem nach Anspruch 13, wobei der lokale transparente VPN-Dienst (102, 401) lokalen VPN-Verkehr für den einen oder die mehreren lokalen Clients (101, 410) abfängt durch Inspizieren von Kommunikationen, die von einem oder mehreren lokalen Clients stammen, unter Verwendung des Sendesteuerungsprorokolls bzw. Transmission-Control-Protocol (TCP) oder des Dateiübertragungsprotokolls bzw. File-Transfer-Protocol (FTP).

17. VPN-Organisationssystem nach Anspruch 13, wobei die Kommunikationen zwischen den lokalen (102, 401) und den fernen (103, 402) transparenten VPN-Diensten mit gegenseitig ausgetauschten Zertifikaten auftreten.

18. VPN-Organisationssystem nach Anspruch 13, wobei das System sich auf einem Server befindet und eine Vielzahl lokaler Clients (410) bedient, die den VPN-Kommunikationen zugeordnet sind.

19. VPN-Organisationssystem nach Anspruch 13, wobei sich das System auf einem einzelnen Client befindet.

20. Computerprogramm, das wenn es auf einem Computer oder in einem Computernetz ausgeführt wird, das Verfahren durchführt, wie es in einem der Ansprüche 1 bis 12 beansprucht wird.

21. Computerprogramm nach Anspruch 20, wenn auf einem Maschinen-zugreifbaren Medium gespeichert.

Revendications

1. Procédé implémenté par ordinateur pour gérer des communications de réseau privé virtuel (VPN), comportant les étapes suivantes :

recevoir (210), au niveau d'un service VPN transparent local (401), une communication provenant d'un client local (410) qui est dirigée vers un client éloigné (420) sur un réseau non sécurisé (415) ;
identifier (220) un VPN associé à la communication ;
transformer (230) la communication en un format crypté pour livraison dans le VPN ;
envoyer (231) la communication transformée du service VPN transparent local (401) via le VPN vers un service VPN transparent éloigné (402), qui gère le trafic VPN pour le client éloigné en déchiffrant et en fournissant la communication transformée au client éloigné ;
caractérisé en ce que ni le client local (410) ni le client éloigné (420) n'est préconfiguré avec des capacités VPN ou un logiciel spécialisé pour traiter des communications VPN, et **en ce que** ladite réception (210) comporte les étapes suivantes :
détecter, au niveau d'un proxy de transfert ou transparent, d'un routeur ou d'un commutateur (401B), la communication du client, local à chaque fois que le client local essaye d'envoyer la communication de manière non sécurisée sur un réseau au client éloigné via un port de communications prédéfini spécifique (401A) ;
intercepter la communication détectée et la diriger (211) du proxy, routeur ou commutateur vers le service VPN transparent local.

2. Procédé selon la revendication 1, comportant en

outre une interaction (221) avec le service VPN transparent éloigné (402) pour gérer des communications supplémentaires entre le client local et le client éloigné via le VPN.

3. Procédé selon la revendication. 2 comportant en outre l'étape de cacher (222) des données reçues du service VPN transparent éloigné (402) dans un cache local pour une livraison accélérée au client local (410).

4. Procédé selon la revendication 1, dans lequel la réception (210) de la communication comporte en outre la réception de la communication dans au moins un format parmi un format, de protocole de transfert de fichiers (FTP) et un format de protocole de commande de transmission (TCP).

5. Procédé selon la revendication 1, comportant en outre une communication avec le service VPN transparent éloigné (402) sur le réseau non sécurisé (415) via un protocole SSL (Secure Sockets Layer) ou un protocole TLS (Transport Layer Security).

6. Procédé selon la revendication 1, comportant en outre les étapes suivantes :

examiner (330) la communication pour déterminer si la communication est une requête de données qui résident dans un cache local (401C), et si c'est le cas, délivrer (331) les données au client local (410), et sinon, localiser (340) un service VPN transparent éloigné (402) associé au VPN, et dans lequel la communication est transformée (342) en des formats utilisés par le VPN, et envoyés de manière sécurisée sur un réseau non sécurisé vers le service VPN transparent éloigné pour livraison (343) au client éloigné (420).

7. Procédé selon la revendication 6, dans lequel l'examen (330) comporte en outre l'établissement (341) de communications sécurisées avec le service VPN transparent, éloigné (402) en utilisant au moins un protocole parmi un protocole SSL et un protocole TLS.

8. Procédé selon la revendication 6, dans lequel l'examen (330) comporte en outre une identification du service VPN transparent éloigné (402) en tant que service qui gère le trafic de VPN pour le client éloigné (420).

9. Procédé selon la revendication 6, comportant en outre les étapes suivantes :

recevoir une communication de réponse provenant du client éloigné (420) via le service VPN transparent éloigné (402), si la communication a été envoyée via le VPN car elle ne pouvait pas être satisfaite à partir du cache local (401C) ;
transformer la réponse sur la base des formats du VPN ; et
délivrer la réponse transformée au client local.

10. Procédé selon la revendication 6 comportant en outre la gestion (321) de communications supplémentaires associées au VPN à partir d'un ou de plusieurs clients locaux différents (410), qui sont adressées entre un ou plusieurs clients éloignés différents (420), dans lequel le service VPN transparent éloigné (402) gère les communications supplémentaires au nom d'un ou plusieurs clients éloignés différents.

11. Procédé selon la revendication 6, dans lequel la réception comporte en outre l'interception (310) de la communication après avoir détecté que le client local transmet la communication avec un protocole de transfert non hypertexte.

12. Procédé selon la revendication 6, comportant en outre l'interaction (341) avec le service VPN transparent éloigné avec des certificats signés mutuellement qui sont échangés entre les services VPN transparent éloigné et local pendant les interactions.

13. Système de gestion (400) de réseau privé virtuel (VPN), dans lequel ni le ou les clients locaux (410) ni le ou les clients éloignés (420) ne sont pré-configurés avec des capacités VPN ou un logiciel spécialisé pour traiter des communications VPN, comportant :

un service VPN transparent local (401) ;
un proxy, routeur ou commutateur avant ou transparent local (401B), adapté pour détecter une communication provenant d'un client local à chaque fois que le client local essaye d'envoyer la communication de manière non sécurisée sur un réseau à un client éloigné via un port de communications local prédéfini spécifique (401A) et adapté pour intercepter la communication détectée et pour la diriger (211) du proxy, du routeur ou du commutateur local vers le service VPN transparent local ;
un service VPN transparent éloigné (402) ;
un proxy de transfert ou transparent éloigné, un routeur éloigné ou un commutateur éloigné (402B), adapté pour détecter une communication provenant d'un client éloigné à chaque fois que le client éloigné essaye d'envoyer la communication de manière non sécurisée sur le réseau à un client local via un port de communications éloigné prédéfini spécifique (402A), et adapté pour intercepter la communication détectée et pour la diriger (211) du proxy, routeur

ou commutateur éloigné vers le service VPN transparent éloigné.

14. Système de gestion de VPN selon la revendication 13, comportant en outre

un cache local (401C) ;

dans lequel un service VPN transparent local (401) intercepte et gère le trafic VPN au nom d'un ou plusieurs clients locaux (410), et dessert des communications de ces clients locaux avec des données dans le cache local (401C), si disponibles, et si les données ne sont pas disponibles dans le cache local, le service VPN transparent local transmet les communications de manière sécurisée au service VPN transparent éloigné pour une livraison et une desserte par un ou plusieurs clients éloignés (420) que le service VPN transparent éloigné (402) gère.

15. Système de gestion de VPN selon la revendication 13, dans lequel le service VPN transparent local (401) et le service VPN transparent éloigné (402) interagissent via au moins un protocole parmi le protocole SSL et le protocole TLS.

16. Système de gestion de VPN selon la revendication 13, dans lequel le service VPN transparent local (102, 401) intercepte le trafic VPN local au nom d'un ou de plusieurs clients locaux (101, 410) en examinant des communications du protocole TCP ou du protocole FTP provenant d'un ou de plusieurs clients locaux.

17. Système de gestion de VPN selon la revendication 13, dans lequel des communications entre les services VPN transparent local (102 et 401) et éloigné (103, 402) se produisent avec des certificats échangés mutuellement.

18. Système de gestion de VPN selon la revendication 13, dans lequel le système réside sur un serveur et dessert une pluralité de clients locaux (410) associés aux communications VPN.

19. Système de gestion de VPN selon la revendication 13, dans lequel le système réside sur un client unique.

20. Programme informatique qui, lorsqu'il est exécuté sur un ordinateur ou un réseau informatique, met en oeuvre le procédé selon l'une quelconque des revendications 1 à 12.

21. Programme informatique selon la revendication 20, lorsque mémorisé sur un support accessible par machine.

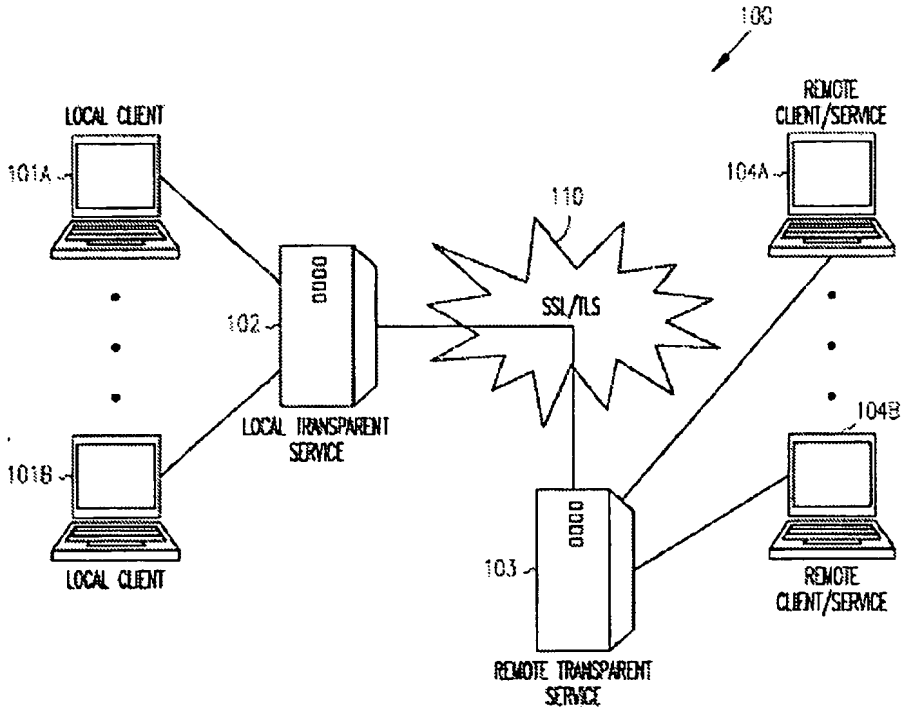
100
LOCAL CLIENT
101A
101B
LOCAL CLIENT
102
LOCAL TRANSPARENT SERVICE
110
SSL/TLS
103
REMOTE TRANSPARENT SERVICE
REMOTE CLIENT/SERVICE
104A
104B
REMOTE CLIENT/SERVICE

FIG. 1

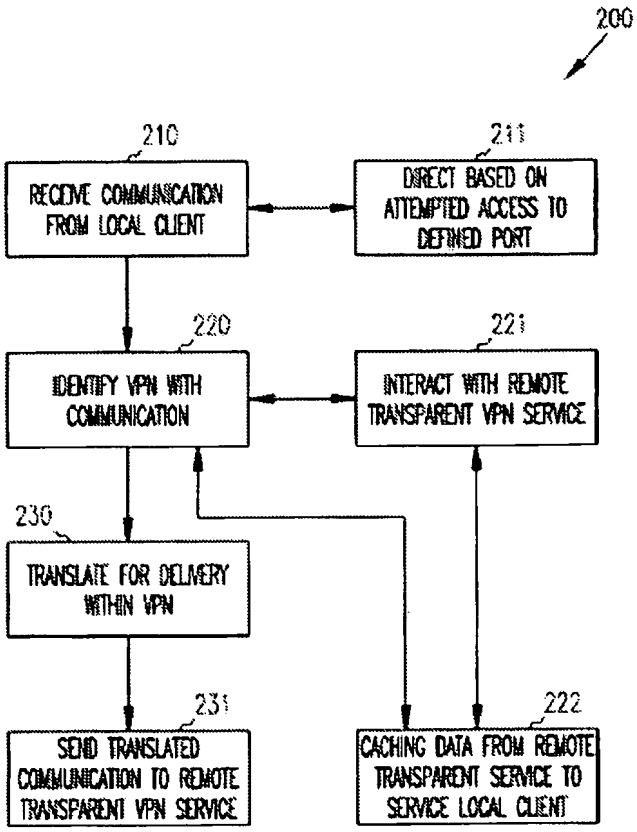
200
210
RECEIVE COMMUNICATION FROM LOCAL CLIENT
211
DIRECT BASED ON ATTEMPTED ACCESS TO DEFINED PORT
220
IDENTIFY VPN WITH COMMUNICATION
221
INTERACT WITH REMOTE TRANSPARENT VPN SERVICE
230
TRANSLATE FOR DELIVERY WITHIN VPN
231
SEND TRANSLATED COMMUNICATION TO REMOTE TRANSPARENT VPN SERVICE
222
CACHING DATA FROM REMOTE TRANSPARENT SERVICE TO SERVICE LOCAL CLIENT

FIG. 2

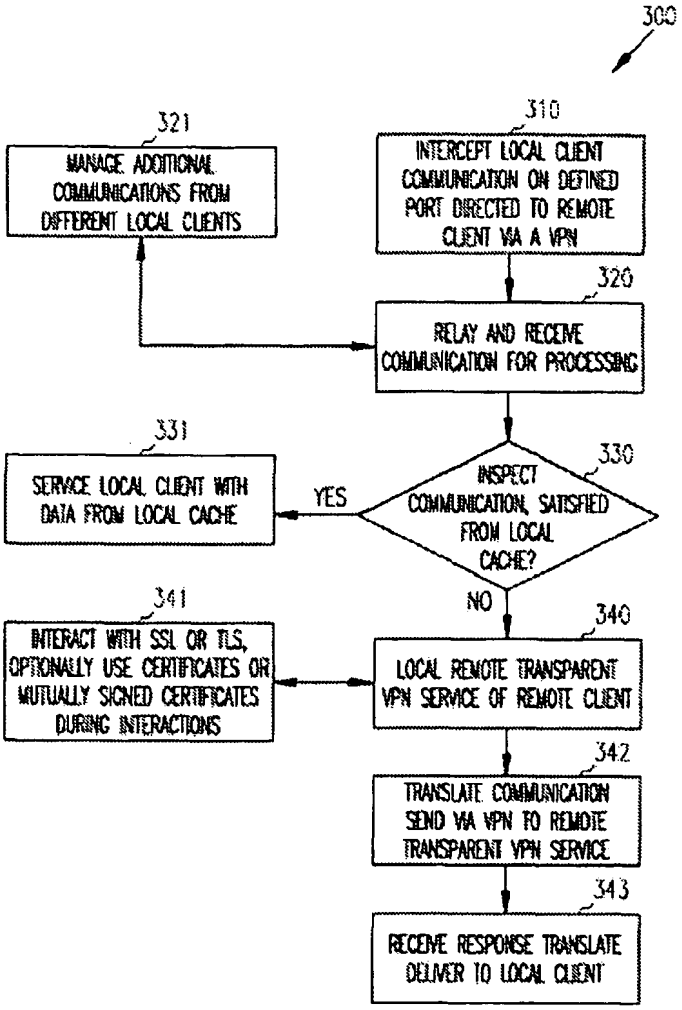
300
310
INTERCEPT LOCAL CLIENT COMMUNICATION ON DEFINED PORT DIRECTED TO REMOTE CLIENT VIA A VPN
320
RELAY AND RECEIVE COMMUNICATION FOR PROCESSING
321
MANAGE ADDITIONAL COMMUNICATIONS FROM DIFFERENT LOCAL CLIENTS
330
INSPECT COMMUNICATION, SATISFIED FROM LOCAL CACHE?
YES
331
SERVICE LOCAL CLIENT WITH DATA FROM LOCAL CACHE
NO
340
LOCAL REMOTE TRANSPARENT VPN SERVICE OF REMOTE CLIENT
341
INTERACT WITH SSL OR TLS, OPTIONALLY USE CERTIFICATES OR MUTUALLY SIGNED CERTIFICATES DURING INTERACTIONS
342
TRANSLATE COMMUNICATION SEND VIA VPN TO REMOTE TRANSPARENT VPN SERVICE
343
RECEIVE RESPONSE TRANSLATE DELIVER TO LOCAL CLIENT

FIG. 3

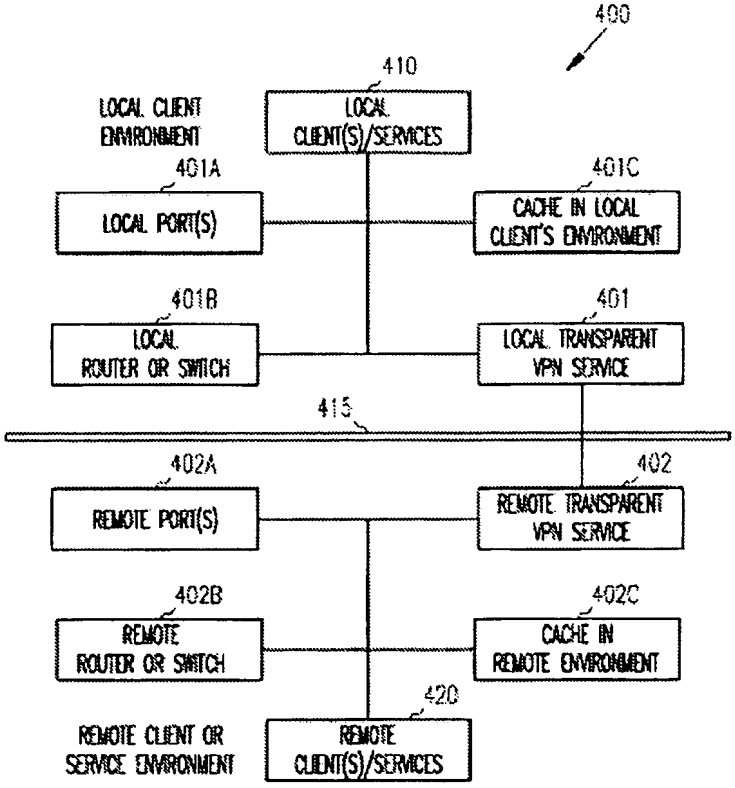
400
410
LOCAL CLIENT ENVIRONMENT
LOCAL CLIENT(S)/SERVICES
401A
LOCAL PORT(S)
401C
CACHE IN LOCAL CLIENT'S ENVIRONMENT
401B
LOCAL ROUTER OR SWITCH
401
LOCAL TRANSPARENT VPN SERVICE
415
402A
REMOTE PORT(S)
402
REMOTE TRANSPARENT VPN SERVICE
402B
REMOTE ROUTER OR SWITCH
402C
CACHE IN REMOTE ENVIRONMENT
420
REMOTE CLIENT OR SERVICE ENVIRONMENT
REMOTE CLIENT(S)/SERVICES

FIG. 4